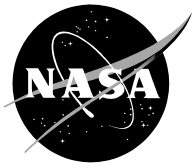

Hold for Release Until
Presented by Witness

National Aeronautics and
Space Administration

September 18, 2020

Subcommittee on Space and Aeronautics

Committee on Science, Space and Technology

U.S. House of Representatives

Statement by:
Jeff Seaton
Chief Information Officer (Acting)

116th Congress
HOLD FOR RELEASE
UNTIL PRESENTED
BY WITNESS
September 18, 2020

Statement of
Jeff Seaton
Chief Information Officer (Acting)
National Aeronautics and Space Administration

before the

Subcommittee on Space and Aeronautics
Committee on Science, Space and Technology
U.S. House of Representatives

Chairwoman Horn, Ranking Member Babin, and members of the Subcommittee, thank you for the opportunity to testify before you today about NASA's information technology (IT) infrastructure, and our efforts to manage and protect this infrastructure during the COVID-19 pandemic while enabling the vast majority of our employees and contractors to continue working remotely. Thankfully, due to strategic Agency investments in the NASA IT environment over the last several years, NASA was well positioned to quickly move its workforce to telework status in early March which not only kept NASA working, but also likely prevented greater exposure of our employees to the highly contagious COVID-19 virus. We are now in the process of returning to more on-site work, in a gradual manner, based on many factors including localized conditions, and guidance from the Centers for Disease Control and other Federal partners. The safety of our workforce remains our top priority. At the same time, protecting and effectively evolving NASA's IT infrastructure continues to be another top Agency focus.

As NASA's Acting Chief Information Officer (CIO), my office provides IT products and services, including policies and procedures for all of NASA. Currently about 17,100 civil servants and 40,000 contractors work at nine NASA Centers and one Federally Funded Research and Development Center, as well as several smaller satellite facilities. We also collaborate with space agencies around the world and have deep partnerships with researchers, engineers, academics, and scientists worldwide. Normally hundreds of thousands of NASA personnel, contractors, partners and members of the public access some part of NASA's IT infrastructure, a complex array of information systems with components geographically dispersed around the globe, on a daily basis. NASA's IT infrastructure plays a critical role in every aspect of NASA's mission, from enabling collaboration to controlling spacecraft to processing scientific data. In the President's FY 2021 budget request, the Agency has proposed to spend approximately $2.2B on enterprise, mission, and mission support IT products and services. NASA also recently received an additional $60M in emergency supplemental funding to help the Agency respond to the COVID crisis, with about one-third of that funding focused on IT capabilities.

Despite the pandemic, NASA remains fully committed to becoming more secure, effective and resilient, and we are actively pursuing these commitments at all levels. Today, OCIO's job is even more challenging with the vast majority of NASA's workforce – both civil servants and contractors – teleworking from remote locations across the country. Thus, enabling the NASA workforce to continue working in an environment that is very different from how we worked only a few months ago, has changed the demands on our IT infrastructure. The requirements and expectations on our IT capabilities and our OCIO teams are high, and the threats from external actors remain an ongoing concern. However,

with hard work, dedication, and innovation, the team I have the privilege of leading has risen to the challenge of keeping NASA's missions moving forward during these challenging times.

The OCIO team, including OCIO employees and contractors at all NASA Centers and facilities, continue to put in long hours, while also developing creative, innovative and secure solutions to new challenges as they arise. One such challenge was the need of NASA's medical community to trace interactions of the NASA workforce with employees who have been confirmed positive for COVID-19 while on-site at any NASA facility. The OCIO team helped develop software that simplified the process of contact tracing conducted by NASA health professionals to protect our workforce and mission while also protecting the privacy information of those exposed, meeting all relevant privacy laws. OCIO has also supported the need for senior leaders to visualize COVID-related data from multiple sources, including regional case-count trends near NASA facilities, thereby enabling senior leaders to make better-informed Return to On-Site Work (RTOW) decisions for each Center across the Agency. During this time, NASA employees as a whole have significantly increased their use of collaboration tools provided by the CIO such as Microsoft Teams and WebEx, as well as secure streaming video for virtual town halls and operational needs. With the support of OCIO, NASA also has continued to hire and onboard new employees and contractors, and to support summer interns with virtual learning opportunities, including providing them with the technology tools they need through both on-site and remote distribution. Even this testimony and various Agency meetings with Congressional Members and staff have been done remotely. During the pandemic, we have seen individuals and teams find new ways to keep the mission moving forward; to support each other; to balance work and family pressures; and even dedicate their expertise and personal time to partner with local companies to help develop technologies to help treat COVID patients and to better protect frontline responders. These are just a few of our success stories – many of which we've shared with other Federal partners. We also continue to learn from the telework experiences of other Federal agencies, fully recognizing that we are all in this together. My testimony today will touch on some of these successes, while also describing NASA's remote work journey, addressing how we are responding to increased requirements on and threats to our IT infrastructure during the pandemic – themes that are common to many Federal agencies.

Responding to a Pandemic

As signs of a nationwide pandemic developed in early February 2020, NASA senior leaders began to use the Agency's Continuity of Operations Plan (COOP) to assess capabilities and conditions at Agency locations and determine when it would be appropriate to proactively begin moving employees into a telework status due to the increasing spread of the virus. Then in early March, NASA conducted an Agency-wide telework exercise to stress test NASA's IT capabilities needed to support massive teleworking. During that exercise, we saw a 300 percent increase in single-day telework users and associated increases in the utilization of our remote IT infrastructure, and our IT systems effectively supported this increased load. Shortly after this exercise, in mid-March, Agency senior leaders began making the difficult decisions to move nearly the entire workforce, Center-by Center based on local conditions, into a telework status. Only a limited number of employees performing mission-critical work requiring on-site access for the protection and safe operation of critical Agency infrastructure and a few select missions (e.g., DM2 launch and Mars Perseverance preparations) were initially authorized to be on-site, following clearly defined health and safety protocols. Thus, NASA has never been "closed." On the contrary, our employees continued to perform NASA's important missions under very difficult personal and professional circumstances, leveraging technology and communication tools to continue a majority of NASA's work. More than 90 percent of the NASA workforce was in a telework status by the end of March 2020. Today, about 75 percent of employees and contractors are continuing to work remotely, with the amount varying by mission requirement and location.

NASA is currently using a NASA-developed RTOW Framework[1] to safely increase the amount of work being done on-site at our Centers and facilities. Increased levels of RTOW will be gradual as local conditions at each NASA Center/facility become safer to return. NASA also has strict safety protocols in place for employees who are returning to on-site work, including requiring all employees (civil servant and contractor) and anyone else who enters a NASA facility to wear face masks when they cannot ensure appropriate social distancing. NASA Centers and facilities are also using temperature checks as a health screening tool, and NASA continues to investigate other technologies that may provide protections for our workforce. Should an employee who has been on-site test positive for COVID-19, NASA has a contact tracing protocol to identify and notify others who may have been exposed to an infected person. NASA then requires infected and exposed persons to self-quarantine, and we have aggressive cleaning protocols for impacted areas. NASA also continues to actively communicate with other Federal agencies about how we are responding to the COVID crisis and to share best practices with them, while also learning from the successes of others.

During these challenging times, NASA senior leadership continues to put our employees first by maximizing flexibilities for employees to perform their NASA work while also enabling them to care for themselves and their families. Leave and telework flexibilities consistent with Office of Personnel Management (OPM) guidance are available to employees, including limited paid leave for care of young children. We also have encouraged our supervisors to provide the greatest amount of flexibility in what hours employees work., e.g., allowing them to change start/stop times or to break up their eight-hour workdays into sections to better accommodate their family needs at home. For my part, even with the increased demands on our IT workforce, I am challenging my team leaders to set the example and take time off to recharge and take care of themselves and their families. We're also encouraging employees to "unplug" and take breaks, which admittedly can be difficult when you work in OCIO and have to keep the Agency's IT infrastructure performing securely 24 hours a day, 7 days a week. NASA also continues to keep our workforce informed about RTOW plans via emails from senior leaders, virtual townhall events, and Agency-wide and Center-specific websites.

The NASA Telework Experience

Over the last several years, NASA has invested significantly in modernizing our network, collaboration tools, and cybersecurity capabilities that are critical to enabling NASA team members to effectively work both on site and remotely. We've also conducted multiple Center and Agency telework exercises to test our systems and to learn from and resolve any issues. The lessons we've learned through our COOP and telework exercises enabled us to rapidly and seamlessly transition into what has become an extended telework environment. Even before the pandemic, the NASA OCIO was analyzing ways to allow for our employees to securely work remotely from any location due to the increasingly mobile nature of our workforce. For many years, NASA has been moving from stand-alone desktops to mobile laptops to support the way in which distributed, mobile teams work. Many employees travel occasionally and/or bring their laptops home with them often – even daily – in case of weather events or other emergencies, or simply to do work in the evening. NASA also supports routine telework. With supervisor approval, it was not unusual for some employees to telework one or two days a week even prior to the pandemic. While some work must always be performed on site, the NASA team has been incredibly productive over the past several months of largely remote work and we are already using the lessons we have been learning during the pandemic to add to our ongoing "Future of Work" planning – a NASA effort where OCIO is playing a key role in helping to define NASA's future work environment.

[1] The following website includes specifics about our RTOW plans; including a copy of our RTOW Framework; a list of Frequently Asked Questions and Answers; and a list of the each Center's operational status: https://nasapeople.nasa.gov/coronavirus/coronavirus.htm.

With most of the NASA workforce teleworking during the pandemic, there are greater risks to NASA data when accessed remotely as opposed to being on site with a direct Agency network connection. To address the increased risks associated with remote work, several years ago, NASA began protecting information on Agency laptops with Data At Rest encryption software. Additionally, NASA IT users who are working remotely are required to use the NASA Virtual Private Network (VPN) when connecting to internal NASA systems. Additionally, NASA OCIO has authorized some missions to host their own VPNs, which allows defined limited connectivity to external partners, thus enforcing segregation our partners and their systems from NASA's internal systems.

Pre-pandemic enhancements to NASA's remote infrastructure also aided its response to the present pandemic. In early 2019, NASA OCIO upgraded the Agency's VPN infrastructure, expanding capacity from 24,000 to more than 55,000 concurrent users. Additionally, NASA OCIO made improvements to its network architecture to add additional resiliency, redundancy, and increased bandwidth. At the height of teleworking during the pandemic, where NASA saw about 90 percent of the workforce connecting remotely, an average of more than 37,000 civil servants and contractors were using the Agency's VPN each day, with the maximum utilization exceeding 40,000 users in a single day. Prior to the pandemic, the most connect ions to the NASA VPN on a single day was less than 12,000. While there have been some minor network and connectivity issues that have required additional architecture and configuration changes during the pandemic, and while we cannot address home and local network issues, the NASA network and VPN infrastructure has performed extremely well, with a measured 99.85 percent availability since the start of the remote telework period.

When working remotely, employees can respond to phone calls via NASA-provided mobile data devices, or by calling into a voicemail system and retrieving messages. In addition, NASA is using a softphone application installed on employee laptops that allows users to use their computers to make and receive phone calls over the network as if using their office telephone. Email and official documents sent on NASA-provided mobile devices are also secured via NASA's mobile device management software which provides secure storage and encrypted mobile connection to NASA mobile applications, including email and scheduling.

During the pandemic, NASA employees have capitalized on new ways to virtually connect and collaborate via tools such as Microsoft Teams, which OCIO finished deploying across NASA in October 2019 as part of the Agency's migration to the Microsoft Office 365 cloud-based suite of tools. While some employees adapted to the new collaboration tools immediately, use of these new capabilities really grew rapidly once NASA employees began working remotely, because they suddenly had a need to conduct meetings and have conversations with colleagues that were also remote. In fact, the video and chat capabilities became such a critical tool for the entire NASA workforce that NASA's use of Teams increased more than 300 percent since March to nearly 38,000 daily active users, and this way of virtually working via video has now become the norm. An additional response to the pandemic-related collaboration needs included NASA's CIO team integrating audio dial-in capabilities with Teams meetings beginning in April, replacing the need for many traditional, external conference-call lines. This audio integration also supported the accessibility needs of the workforce by allowing interpreters to use the dial-in functionality during meetings. As of August, NASA has approximately 9,000 employees using the new Teams audio-conference capability, providing them access to virtual team meetings even if their only access is a mobile phone. In parallel, OCIO expedited the release and availability of mobile Office 365 applications for NASA-managed mobile phones, so that employees can also connect to Teams meetings and access video and chat from their mobile phones via a Wi-Fi or cellular data connection, making many employees truly mobile NASA workers. Also, the recent addition of live captioning to Teams meetings further expanded the accessibility capabilities provided to NASA employees.

Providing new and replacement equipment and effective remote support has been essential to sustaining the productivity of the remote NASA workforce during the pandemic. To address these challenges, NASA OCIO developed and implemented a process to ship IT equipment (laptops, cell phones) to new employees, as well as replacement hardware to current employees experiencing technical difficulties and system failures, and established processes to set up, configure, and remotely troubleshoot hardware and software remotely. These processes have allowed employees to remain safely at home and avoid visits to a NASA Center to resolve technical issues in person, although on-site support is also available when needed. OCIO also partnered with the Office of Protective Services (OPS) to implement a secure approach to remotely process personal identity verification (PIV) badge renewals and replacements utilizing the expanded collaboration capabilities, again allowing employees to avoid travelling to a NASA Center unnecessarily. This activity involved collaboration with multiple offices including OPS and the Office of the Chief Human Capital Officer. Additionally, OCIO increased staffing at IT help desks to assist employees who were experiencing technical difficulties, in most cases, completely virtually.

NASA IT Threat Environment

Like other Federal agencies, NASA's IT infrastructure is under constant attack from domestic and foreign adversaries. Decades of NASA aeronautics and space technology research and development represents billions of dollars in U.S. Government and aerospace industry investment. The very nature of NASA's mission, and the extremely important technical and intellectual capital produced therein, makes the Agency's information a valuable target for hackers, criminals, and foreign enterprises. Many of these threats are well-resourced, highly motivated, and sophisticated – and those threats have not gone away during the pandemic. Unfortunately, there is no perfect, one-size-fits-all approach or technology to predict, counter, and mitigate the wide range of cyber attacks across the Federal Government. To address this dynamic threat landscape, NASA continues to strengthen our technical and procedural capabilities to attain situational awareness and proactively defend the IT assets supporting our enterprise, including those assets that are outside the traditional borders of the NASA network.

The collective actions of the NASA OCIO team, as well as information sharing with the Department of Homeland Security (DHS) and other Federal agencies involved in cybersecurity, are contributing to an improved IT security posture at NASA. When threats are detected, NASA personnel take immediate action and depending on the level of the threat, NASA alerts other Federal agencies involved with cyber intelligence issues, and partners with them to deter and thwart future attacks. Today, for example, NASA is a leader in the adoption of DHS's Continuous Diagnostics and Mitigation (CDM) program, which enables NASA to identify assets and vulnerabilities across our network and implement plans for remediation of issues. We have partnered with other agencies that have deployed CDM to ensure we can transfer our knowledge to them, and receive lessons learned from other agencies. Deployment of CDM Phase 1, which focuses on identifying what is on NASA's networks, is now complete across our corporate network and NASA is making significant progress on the mission network, with completion scheduled for the fourth quarter of FY 2021. OCIO has successfully implemented CDM Phase 2, which included identifying "who" is on NASA's network along with privilege access. For CDM Phase 3, which focuses on "network security management" is being worked with DHS as part of the Dynamic and Evolving Federal Enterprise Network Defense (DEFEND) contract. OCIO is currently on schedule with DHS in its deployment of technologies to monitor unauthorized IT device connections designed to remove or block these devices from accessing NASA's networks and systems. OCIO's initial enforcement implementation for the corporate network is scheduled for the second quarter of FY 2021. While NASA's cybersecurity efforts will never be "done," significant progress has been made recently. OCIO's efforts to better secure NASA data and systems have resulted in NASA achieving a rating of "Managing Risk," which is the highest rating, on the two most recent Federal Information Security Management Act (FISMA) framework assessments.

In order to address the unique cyber risks and challenges posed by human spaceflight, and in particular by NASA's Artemis Program, OCIO also has partnered with the Human Exploration and Operations Mission Directorate (HEOMD) and its Advanced Exploration Systems Division at Headquarters. A senior OCIO staff member is engaged in program planning and leadership meetings, providing immediate OCIO input on relevant cybersecurity and programmatic matters. This partnership allows OCIO to better understand HEOMD's programs, processes, and mission requirements while helping HEOMD leadership identify and resolve any cybersecurity gaps by evaluating cybersecurity requirements, ensuring an integrated approach to addressing cybersecurity risks, and making certain that cybersecurity considerations are included at the outset of this groundbreaking work. In addition to OCIO's partnership with HEOMD, OCIO continues to proactively work with other NASA projects and missions to strengthen mission cybersecurity and to support emerging IT requirements.

Over the last several years, NASA has also made great strides in PIV efforts, requiring 100 percent of privileged users to authenticate with PIV, and between FY 2017 and FY 2019, increasing the percentage of unprivileged users required to use PIV from 72 percent to 90 percent over that period. NASA has developed PIV solutions for a variety of unique NASA systems and CDM efforts, including developing the first-ever native smartcard authentication for Apple's MacOS platform, a solution which NASA has shared with other Federal partners and further solidifying the security of identity management and access on the Agency's network. Because of these efforts, NASA's Identity, Credential and Access Management (ICAM) program was a finalist for the National Security Agency's prestigious Frank B. Rowlett Award, which recognizes outstanding Federal Government excellence in the field of cybersecurity. This has helped NASA achieve the "Managing Risk' (highest score) under the FISMA framework.

To further strengthen NASA's existing Security Operations Center (SOC), in FY 2020, NASA developed a SOC COOP capability. Previously, if cybersecurity operations at NASA's Ames Research Center were disrupted, the Agency would have been limited in its ability to identify, detect, and respond to cybersecurity incidents. With the new SOC back-up operations and processes in place concurrently across multiple Centers, NASA is prepared to maintain SOC operations in the event of an isolated disruption. The development of the SOC COOP was accompanied by an increase in NASA's overall SOC capabilities as well, moving the NASA SOC from a predominately reactive capability to a pro-active resource supporting the Agency's cybersecurity needs. As the pandemic spread in April, 2020, NASA OCIO made the decision to activate our previously-established and tested COOP plan and moved our 24x7 network operations center which manages NASA's critical administrative network infrastructure to a remote operations posture to ensure the safety of NASA's essential network management personnel without impacting services. In this demanding environment, the NASA CIO team has continued to effectively manage and protect NASA's IT infrastructure, largely in a remote manner. On occasions when employees are required to be onsite to support critical SOC or network operations activities, we have followed NASA processes to maintain appropriate social distancing, wear masks as required, and follow all other facility-access requirements.

Despite OCIO's increased workload during the pandemic, the OCIO team also has continued to make progress on several key network and cybersecurity initiatives. For example, to support large, virtual meetings, OCIO deployed a secure, PIV-enabled streaming video service in less than 60 days to support NASA management's need to engage in live communication with employees.

Looking Ahead

Effective IT management in a complex environment like NASA is not an easy task even under normal circumstances. Investment decisions must balance multiple stakeholder and mission requirements, cybersecurity risk management, and the rapid pace of technology development to allocate available

resources to the highest priority IT investments that will best enable mission success. Additionally, like all Federal agencies, NASA is adjusting to new laws and directives designed to improve how the entire Federal Government manages and secures its IT resources. While NASA is proud of the progress we have made, we recognize that more work remains as we strive to effectively and efficiently manage our IT resources, modernize out IT environment, all the while complying with ever-changing laws and policy. There is a lot at NASA to be excited about, and as the Acting CIO, I am encouraged by the continual support the CIO receives from NASA leadership as well as the partnership role the CIO plays in key decision-making processes within the Agency. Here are just a few of the exciting opportunities ahead of the NASA OCIO team:

- **Cloud Computing and Backup:** NASA's commercial cloud computing interest and adoption has rapidly escalated as missions are aggressively making the transition from traditional Agency-hosted software platforms to reliance on cloud-native services and applications. There is also significant interest in delivering observation data from orbiting assets directly to the cloud. NASA is presently consuming more than 1.8M computing hours in the commercial cloud every month and has almost 10 petabytes of data stored in the cloud, with the majority of data available for unrestricted use by the global science community. The portfolio of data for just one major NASA program will increase this data amount by at least an order of magnitude within the next five years. Mission growth in the use of commercial cloud computing services is fully aligned with the Agency's thrust to rely on industry as much as possible for capabilities so that NASA can focus on its key objectives in the areas of science and discovery. Additionally, OCIO is implementing an Agency-wide Cloud Backup Solution in order to seamlessly protect, back up, and restore files across any organization or user, regardless of device or location, from a secure, cloud architecture, a capability that also further protects NASA from growing cyber threats such as ransomware attacks.
- **Website Consolidation and Modernization:** NASA OCIO is also collaborating on a full assessment of NASA's web footprint and digital presence through the NASA Website Modernization Team, which will deliver an enhanced cyber posture, improved operating efficiencies, and a strengthened focus for publicly communicating the inspiring messages and amazing data coming from NASA missions. This is a priority for NASA's senior leadership, as outlined in a May 15, 2019, memo from NASA Administrator James Bridenstine.
- **Digital Transformation:** As part of the NASA CIO's efforts in IT modernization, OCIO is helping to drive the concept of digital transformation across NASA in areas such as collaboration, artificial intelligence and machine learning, cloud computing, big data, and robotic process automation.

Conclusion

In conclusion, NASA is continuing to execute a diverse portfolio of exciting and challenging missions on a daily basis, even with a significant percentage of the NASA team continuing to primarily operate in a remote work environment today. While we are unsure what the future holds in terms of an end to this global pandemic, NASA senior leaders, including myself, are committed to keeping the NASA workforce safe and to providing them with the tools and IT infrastructure they need to continue to successfully execute their missions while working remotely as we gradually return to on-site work. At the same time, I want to assure you that protecting and evolving NASA's IT infrastructure is and will remain a top Agency priority. Thank you for the opportunity to testify before you today and for your continued support of NASA's missions and our people. I would be happy to answer any questions you may have.

Jeff Seaton
NASA Chief Information Officer (Acting)

Jeff Seaton is NASA's Chief Information Officer (Acting). Prior to this appointment, he served as Deputy Chief Information Officer. Seaton came to NASA Headquarters from NASA's Langley Research Center, where he was Chief Information Officer from 2011 to 2018. During that time, he was also a member of the NASA Langley Senior Staff and the Agency's CIO Executive Council. Jeff led transformative change efforts in both the Langley and CIO enterprise across the Agency to increase effectiveness and accountability of the services provided by the organization.

Jeff began his career with NASA in 1991 as a research engineer designing robotic systems for use in space-based applications. He also conducted research in the field of computer vision techniques applied to the control of robots. Jeff was a member of NASA's 2008 Senior Executive Service Candidate Development Program and served as Langley's Chief Technology Officer and Deputy Chief Information Officer prior to becoming CIO.

In addition to his CIO duties, Jeff was a member of the Business Services Steering Committee charged with identifying opportunities for NASA to improve the efficiency and effectiveness of all mission support services. He was also the executive champion of the Langley Emerging and Advancing Professionals employee resource group, has led Langley's digital transformation efforts, and helped to lead Langley's High Performance Computing Incubator. He has received numerous awards for his service to the Agency, including NASA's Outstanding Leadership Medal in 2014.